

# **FORSKRIFTER FOR SALG MOT BETALNING MED KONTOKORT**

*Distansehandel (Card not Present)*

**(S6 - juli - 2008)**

*Disse forskriftene, "Distansehandelsforskriftene", gjelder for salg mot betaling med Kontokort ved Distansehandel. Med "Distansehandel" forstås Salgsmåte der Kontokort ikke er tilstede ved betalingen. De "Salgsmåter" som omfattes av Distansehandelsforskriftene, er f.eks salg over Internett, salg mot post- og/eller telefonordre, mobilbetalinger og Tilbakevendende Betalinger. Med "Tilbakevendende Betalinger" forstås s.k. abonnementsbetalinger der kortinnehaveren aksepterer at Salgsselskapet løpende kan belaste Kontokortet ved tilbakevendende fremtidige tilfeller (f.eks abonnemeter).*

*Distansehandelsforskriftene utgjør et tillegg til Vilkår for innløsning av kontokorttransaksjonerr ("Hoveddokumentet") som er inngått mellom Salgsselskapet og Euroline. Ved eventuell motstrid mellom Hoveddokumentet og Distansehandelsforskriftene skal Distansehandelsforskriftene gå foran.*

## **1. Generelt om salg mot betaling med Kontokort ved Distansehandel**

Ved Distansehandel er Kontokortet ikke fysisk tilstede, og Salgsselskapet kan dermed ikke identifisere kortinnehaveren på samme måte som når Kontokortet er tilstede. Salgsselskapet har derfor alltid, med de begrensninger som kan følge av punkt 6 nedenfor, risikoen for samtlige kjøpstransaksjoner ved Distansehandel. Dette innebærer at Euroline har rett til å tilbakebelaste Salgsselskapet beløp som kortinnehavere protesterer mot. Dette gjelder uansett om kortinnehaverens innvending er berettiget eller ikke.

## **2. Særskilte tiltak ved Distansehandel**

Salgsselskapet forplikter seg til å:

- tydelig informere kortinnehaveren på bestillingsformularet eller internettsiden innen betalingsinstruksjonene om hvilket land Transaksjonen skjer samt i hvilket land Salgsselskapet betaler merverdiavgift.
- ikke legge sammen Transaksjoner uten særskilt tillatelse fra Euroline, dvs. ikke skape 1 (en) Transaksjon gjennom å sammenfatte flere Transaksjoner.

## **3. Kontroller**

Salgsselskapet skal ved debitering av kortinnehaveren utføre de nedenfor angitte kontroller:

### **3.1 Godkjennelse**

Godkjennelse skal alltid skje på betalingstidspunktet, uansett kjøpsbeløp. Godkjennelsen må kodes med korrekt Salgsmåte. De koder som skal anvendes i denne forbindelse fremgår av Instruksjonene.

### **3.2 Adressekontroll**

Adressekontroll skal utføres i henhold til Instruksjonene i den utstrekning som angis i bilag til Hoveddokumentet. Adressekontroll innebærer kontroll av at ønsket leveringsadresse er i samsvar med den adresse som kortinnehaveren har oppgitt til kortutstederen. Dersom godkjennelse av en kjøpstransaksjon skjer elektronisk, skal det på bestillingsunderlaget for adressekontroll tydelig angis "Kun adressekontroll". Adressekontroll gjelder bare for post- og/eller telefonordre.

### **3.3 Sikkerhetskode**

Kontroll av sikkerhetskoder skal utføres i henhold til Instruksjonene i den utstrekning som angis i bilag til Hoveddokumentet. Kontroll av sikkerhetskoder innebærer at den sikkerhetskoden som normalt finnes nederst i signaturfeltet på Kontokortets bakside, undertiden kalt CVV2 eller CVC2, er i samsvar med den sikkerhetskoden som finnes hos kortutstederen. Salgsselskapet må ikke under noen omstendigheter lagre sikkerhetskoden.

## **4. Ordreformular/bestillingsunderlag**

### **4.1 Innhold**

Salgsselskapets ordreformular/bestillingsunderlag skal være stilet til Salgsselskapet og inneholde:

- Salgsselskapets navn, sted og organisasjonsnummer
- kortinnehaverens navn
- kortinnehaverens adresse (leveringsadresse)
- Kontokortets nummer og gyldighetstid
- bestillingsdato
- bestillingens beløp
- opplysninger om merverdiavgift

#### **4.2 Lagring**

Salgsselskapet skal i 18 (atten) måneder arkivere ordreformularer/bestillingsunderlag. På Euroline anmodning skal Salgsselskapet innen 5 (fem) bankdager overlevere ordreformular/bestillingsunderlag som gjelder enkelttransaksjoner.

#### **4.3 Kortinnehaverens kvittering**

Kortinnehaveren skal alltid motta kvittering for bestilt vare eller tjeneste fra Salgsselskapet. I gitte tilfeller, f eks ved salg over Internett, skal Salgsselskapet sende en elektronisk kvittering til kortinnehaveren med den informasjon som angis i punkt 5.2 nedenfor.

### **5. Regnskap**

#### **5.1 Innsendelse av kjøpstransaksjoner m.m.**

Elektronisk innsamlede kjøpstransaksjoner skal senest innen 2 (to) dager fra dagen for betalingen overføres til Euroline. I de tilfeller det forekommer papirkvitteringer, f eks ved post- og/eller telefonordre, skal de være Euroline, eller den Euroline angir, ihende senest 5 (fem) dager fra dagen for betalingen. "Dagen for betalingen" er dagen for godkjenningen.

Ved Tilbakevendende Betalinger skal Salgsselskapet overføre til Euroline Salgsselskapets URL og/eller telefonnummer i kjøpstransaksjonen i henhold til Instruksjonene.

Kjøpstransaksjoner skal leveres til Euroline i henhold til den til enhver tid avtalte rutine. Kjøpstransaksjonene skal ikke overføres til Euroline for innløsning før levering av varen eller tjenesten er påbegynt. Med levering av tjeneste menes også at bindende avtale er inngått om vedkommende tjeneste som skal leveres/utføres senere. Levering kan ved post- og/eller telefonordre, dersom ikke annet er skriftlig avtalt, bare skje til den adresse som kortinnehaveren har oppgitt til sin kortutsteder.

#### **5.2 Transaksjonsinformasjon og logg**

Salgsselskapet skal for hver Transaksjon med Kontokort registrere følgende Transaksjonsinformasjon i en elektronisk Transaksjonslogg:

- Salgsselskapets navn og kundenummer hos Euroline
- Salgsselskapets URL (bare ved Internettbestilling)
- valuta og beløp
- oppgave over merverdiavgift
- dagen for betalingen (for Transaksjoner som gjelder betaling for en reise, et arrangement e.l., som skal finne sted på et fremtidig tidspunkt, skal også dagen for reisens, arrangementets o.l. gjennomføring angis)
- unikt Transaksjonsnummer
- kortinnehaverens navn og eventuelt kundenummer hos Salgsselskapet
- kontrollnummer som bevis for godkjenning
- Transaksjonstype (betaling eller retur/kreditering) i klartekst
- Beskrivelse av kjøpte/returnerte varer/tjenester
- Kontokortets nummer i kryptert eller trunkert form
- Kontokortets gyldighetstid i kryptert form
- Betalingsmåte (se punkt 4.1 annet avsnitt ovenfor)

### **6. Særskilt om salg over Internett**

Ved salg over Internett skal 3D Secure, dvs. Verified by Visa henholdsvis MasterCard SecureCode, anvendes i henhold til Instruksjonene.

Når 1) Salgsselskapet har implementert 3D Secure, 2) Salgsselskapet har kodet Transaksjonene i henhold til Instruksjonene, og 3) kortinnehaveren har autentisert seg mot sin kortutsteder, har Euroline ikke rett tilbakebelaste omtvistede beløp som det protesteres mot som bedragerske eller urettmessige kjøp.

Visa og MasterCard kan også til enhver tid bestemme at Euroline, til tross for at kortinnehaveren ikke har autentisert seg mot sin kortutsteder, ikke har rett til å tilbakebelaste omtvistede beløp som det protesteres mot som bedragerske eller urettmessige kjøp.

Når det gjelder beløp som det protesteres mot av annen grunn enn som bedragerisk eller urettmessig kjøp, har Euroline rett til å tilbakebelaste i henhold til punkt 1 ovenfor selv om Salgsselskapet har implementert 3D Secure.

Visse av MasterCards og Visas produkter samt utenlandske kort har for tiden ikke støtte for 3D Secure.

Salgsselskapet skal også vise logotypene for Verified by Visa og MasterCard SecureCode på betalingssiden/kassasiden.

Punkt 6 i Hoveddokumentet gjelder selv om Salgsselskapet har implementert 3D Secure.

## **7. Sikkerhet**

### **7.1 Håndtering av informasjon om Kontokort**

For dels å beholde et høyt sikkerhetsnivå i de globale kortbetalingssystemene, dels å styrke tilliten til Kontokort som betalingsmiddel, er det av ytterste viktighet at alle som håndterer informasjon om Kontokort gjør det på en sikker måte. Av denne grunn har kortbransjen blitt enige om en felles standard for håndtering av kortinformasjon. Standarden kalles Payment Card Industry (PCI) Data Security Standard (DSS) og er utviklet av de internasjonale kortnettverkene Visa og MasterCard.

Salgsselskapet forplikter seg til å følge standarden PCI DSS i den utgave den til enhver tid finnes offentliggjort i på [www.pcisecuritystandards.org](http://www.pcisecuritystandards.org).

Dette innebærer bl.a. at Salgsselskapet:

- ikke under noen som helst omstendigheter må lagre eller skrive ut i) CVV/CVC (dvs. kortverifiseringsverdien i Kontokortets magnetstripe), ii) CVV2/CVC2 (dvs. den sikkerhetskode som normalt finnes i slutten av signaturfeltet på Kontokortets bakside) eller iii) iCVV/iCVC (dvs. verifiseringsverdien i et Kontokort som er utstyrt med chip). Salgsselskapet forplikter seg også til ikke å lagre eller skrive ut PVV (dvs. verifiseringsverdien for PIN-koder)
- bare kan lagre slik informasjon om Kontokortet som er absolutt nødvendig for Salgsselskapets virksomhet (dvs. navn, Kontokortets nummer og Kontokortets gyldighetstid)
- må oppbevare/lagre media som inneholder informasjon om Kontokortet (f eks logger, Transaksjonsrapporter, elektroniske kvitteringer eller avtaler) på et sikkert sted og på slik måte at bare personer som har behov for tilgang til vedkommende materiale gis slik tilgang
- må håndtere all informasjon om Kontokort konfidensielt og ikke meddele utenforstående noe om de personopplysninger (f eks navn og personnummer) som Salgsselskapet kan komme i besittelse av
- må oppbevare informasjon om Kontokortets nummer på slik måte at ingen uberettiget bruk kan forekomme
- må påse at elektroniske kvitteringer og andre medier er beskyttet mot uberettiget tilgang

- umiddelbart melder fra til Euroline dersom Salgsselskapet oppdager, eller har mistanke om, at informasjon om et Kontokort er brukt på uberettiget måte eller på annen måte er misbrukt. Ved mistanke om misbruk skal Salgsselskapet på Eurolines anmodning også politianmelde hendelsen
- må påse at Kontokortets nummer ikke vises for andre personer enn de personer hos Salgsselskapet som har behov for tilgang til det
- må påse at det dokumenteres hvordan informasjon om Kontokort beskyttes i Salgsselskapets tekniske utstyr
- må påse at det finnes rutiner for sikker Håndtering og distribuering av følsom informasjon om Kontokort og at disse rutinene regelmessig følges opp og kontrolleres. Rutinene, eller informasjon om dem, skal ødelegges på sikker måte, f eks ved hjelp av makuleringsmaskin, når rutinene/informasjonen ikke lenger behøves i henhold til gjeldende lovgivning og/eller Instruksjonene
- må påse at det finnes en fortegnelse over alt teknisk utstyr og at dette utstyret oppbevares på sikker måte
- må påse at informasjon om Kontokort og/eller kortinnehaver gjøres ubrukbar så snart teknisk utstyr og/eller annet medium som inneholder slik informasjon ikke lenger skal anvendes av Salgsselskapet

## **7.2 Godkjennelse av system**

Systemer som leverer Transaksjoner til Euroline må være godkjent av Euroline eller av tredjepart som Euroline utpeker. Euroline kan stille krav om særskilt undersøkelse av følsomme komponenter fra et sikkerhetsmessig synspunkt. Denne undersøkelsen eller skanning utføres av en aktør utpekt i samråd med Euroline.

## **7.3 Særskilt om s.k. Noder og Payment Service Providers**

Anvender Salgsselskapet en tredjepart (s.k. node eller Payment Service Provider) for deler av eller all Distansehandel, må Salgsselskapet sikre at denne oppfyller alle krav i henhold til PCI DSS

## **7.4 Endringer i systemer m.m.**

Endringer i systemet som påvirker de forutsetninger som gjaldt på tidspunktet for godkjennelse må ikke foretas uten Euroline godkjennelse.

Salgsselskapet skal gjennomføre en test anvist av Euroline av oppkoblingen mot Eurolines mottakssystem før Transaksjoner kan innsendes til Euroline.

## **7.5 Sikkerhetsregler**

Salgsselskapet må påse de Sikkerhetsregler som til enhver tid er fastsatt av Euroline følges.

## **7.6 Dataintrengning og IT-teknisk undersøkelse**

Dersom Euroline har mistanke om at Salgsselskapets kassesystem, datasystem e.l. er utsatt for inntrengning, manipulasjon e.l. som etter Eurolines mening på noen måte berører Partenes samarbeid i henhold til denne Avtale, har Euroline rett til å gjennomføre en s.k. IT-teknisk undersøkelse ("Undersøkelsen") av vedkommende utstyr. Undersøkelsen kan gjennomføres av Euroline eller av et IT-teknisk foretak engasjert av Euroline.

Tidspunkt, og spørsmål/rutiner i den forbindelse som gjelder gjennomføringen av Undersøkelsen, skal dersom Euroline ikke anser det som uegnet, i størst mulig utstrekning avtales mellom Partene. Euroline har allikevel rett til, dersom det etter Eurolines mening er mest formålstjenlig, å besøke Salgsselskapet og gjennomføre Undersøkelsen uten at Salgsselskapet på forhånd underrettes om dette.

Det påligger Salgsselskapet i rimelig utstrekning å medvirke ved Undersøkelsen og lette gjennomføringen slik at hensikten med Undersøkelsen, dvs. å fastslå hvordan inntrengning /manipulasjon har skjedd, kan oppnås.

Dersom det gjennom Undersøkelsen konstateres at Salgsselskapets kassesystem, datasystem e.l. har vært utsatt for inntrengning, manipulasjon e.l., skal Salgsselskapet på Eurolines anmodning erstatte Euroline kostnadene for Undersøkelsen.